262 Bkk, Immeuble LOGEX Lomé – TOGO
Tél: +228 90 77 02 52 / 90 08 39 69 / 96 05 01 21
Email: info@cybsol.biz | site web: www.cybsol.biz

INTRODUCTION À LA CYBERSÉCURITÉ (INCSv1)

OBJECTIF

L'objectif général de cette formation en introduction à la cybersécurité est de fournir aux participants les connaissances de base nécessaires pour comprendre les principes fondamentaux de la cybersécurité et les préparer à prendre des mesures pour protéger les systèmes et les données contre les menaces informatiques. Cette formation constitue une excellente première étape pour démarrer une carrière en cybersécurité en fournissant une base solide de connaissances et de compétences.

En complément à cette formation, d'autres formations spécialisées peuvent être envisagées pour approfondir les domaines spécifiques de la cybersécurité. Pour plus de détails se référer à notre catalogue de formations ou notre site web https://cybsol.biz

Ces formations complémentaires, combinées à la formation en introduction à la cybersécurité, fourniront aux participants une base solide pour démarrer une carrière en cybersécurité. La combinaison de connaissances théoriques et pratiques acquises tout au long de ces formations permettra aux participants de se positionner comme professionnels compétents dans le domaine de la cybersécurité et d'ouvrir des opportunités d'emploi dans ce secteur en pleine croissance.

SYLLABUS :

1. Introduction à la cybersécurité

- Définitions et concepts de base : Les participants apprendront les termes et concepts clés tels que les menaces, les vulnérabilités, les risques, etc.
- Importance de la cybersécurité : Les participants comprendront pourquoi la cybersécurité est essentielle dans le monde numérique actuel en explorant des exemples d'incidents de sécurité et leurs conséquences.

- Menaces et attaques courantes : Les participants étudieront les différentes menaces et attaques auxquelles sont confrontés les systèmes informatiques, tels que les logiciels malveillants, l'ingénierie sociale, etc.

2. Fondamentaux de la sécurité informatique

- Principes de base de la sécurité des systèmes d'information : Les participants découvriront les principes fondamentaux de la sécurité, tels que la confidentialité, l'intégrité et la disponibilité des données.
- Authentification, autorisation et contrôle d'accès : Les participants apprendront comment mettre en place des mécanismes d'authentification solides.

3. Législation et réglementation en matière de cybersécurité

- Les participants comprendront les lois et réglementations relatives à la cybersécurité afin de se conformer aux exigences légales (par exemple, la norme ISO 27001)
- Méthodes pour évaluer et assurer la conformité légale en matière de cybersécurité
- Éthique professionnelle dans le domaine de la cybersécurité : Les participants seront sensibilisés aux problèmes éthiques liés à la cybersécurité.

4. Gestion des risques

- Définition des risques informatiques et de leur impact potentiel : Les participants comprendront ce que sont les risques informatiques et comment ils peuvent affecter les systèmes informatiques et les données sensibles.
- Présentation des méthodes d'analyse des risques : Les participants seront initiés aux bases de l'analyse qualitative et quantitative des risques
- Présentation des différentes approches de gestion des risques : Les participants apprendront à choisir la meilleure approche de gestion des risques en fonction du contexte organisationnel, des ressources disponibles et des objectifs de sécurité.

5. **Sécurité des réseaux**
    - Architecture et protocoles réseau : Les participants comprendront les principes de base de l'architecture réseau et étudieront les protocoles couramment utilisés.
    - Détection d'intrusion et prévention des intrusions : Les participants exploreront les techniques utilisées pour détecter et prévenir les intrusions dans les réseaux.

6. **Cryptographie et sécurité des données**
    - Principes de base de la cryptographie : Les participants étudieront les principes de base de la cryptographie, y compris le chiffrement symétrique et asymétrique.
    - Chiffrement des communications : Les participants découvriront comment sécuriser les communications en utilisant des protocoles cryptographiques tels que SSL/TLS.
    - Sécurité des données : Les participants apprendront comment protéger les données sensibles en utilisant des mécanismes de chiffrement et d'autres techniques de protection des données.

7. **Sécurité des applications web**
    - Vulnérabilités courantes des applications web : Les participants examineront les vulnérabilités courantes des applications web telles que les injections SQL, le cross-site scripting (XSS), etc.
    - Bonnes pratiques de développement sécurisé : Les participants seront sensibilisés aux bonnes pratiques de développement sécurisé pour éviter ces vulnérabilités.
    - Tests de sécurité des applications web : Les participants apprendront à effectuer des tests de sécurité sur les applications web pour identifier les vulnérabilités et proposer des correctifs.

8. **Gestion des incidents de sécurité**
    - Détection, analyse et réponse aux incidents de sécurité : Les participants découvriront les processus de détection, d'analyse et de réponse aux incidents de sécurité pour minimiser les dommages potentiels.

- Planification de la continuité des activités et reprise après sinistre : Les participants apprendront à élaborer des plans pour maintenir la continuité des activités en cas d'incident de sécurité majeur.

9. Sensibilisation à la sécurité

- Bonnes pratiques d'utilisation d'Internet et des dispositifs numériques : Les participants recevront des conseils sur les bonnes pratiques d'utilisation d'Internet et sur la protection des dispositifs numériques personnels.
- Phishing, hameçonnage et autres techniques d'ingénierie sociale : Les participants seront conscients des différentes techniques utilisées par les attaquants pour tromper les utilisateurs et voler leurs informations.
- Formation sur la sensibilisation à la sécurité pour les utilisateurs : Les participants apprendront comment sensibiliser les utilisateurs aux bonnes pratiques en matière de sécurité informatique.

10. Cloud

- Définition et principes du Cloud Computing : Connaître les principes de base du Cloud Computing tels que l'accès à la demande via Internet, l'élasticité des ressources et la mutualisation des ressources
- Avantages et inconvénients de l'utilisation du Cloud : Être conscient des inconvénients potentiels tels que les préoccupations en matière de sécurité et de confidentialité des données
- Les défis de sécurité spécifiques au Cloud Computing : Comprendre les risques tels que la perte de contrôle des données, les attaques de type "multi-locataire" ou les problèmes de conformité réglementaire.
- Mesures de sécurité pour protéger les données et les systèmes dans le Cloud : Connaître les mesures telles que le chiffrement des données, la gestion des identités et des accès, la surveillance des activités suspectes et la sauvegarde régulière des données.

11. Examen final (Note de passage : 70%)